3

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/808,530	03/14/2001	James Riordan	CH920000013US1	3810

7590 09/08/2004

Louis P. Herzberg
Intellectual Property Law Dept.
IBM Corporation
P.O. Box 218
Yorktown Heights, NY 10598

EXAMINER	
KLIMACH, PAULA W	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 09/08/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/808,530	**Applicant(s)** RIORDAN, JAMES	
	Examiner Paula W Klimach	**Art Unit** 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _30 July 2001_.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-13_ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-13_ is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _07/30 and 06/11_.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .
5) □ Notice of Informal Patent Application (PTO-152)
6) □ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

Claims 1, 6, and 8-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Guski et al (5,592,553) in view of Abadi et al (6,141,760).

In reference to claims 1 and 8-10, Guski discloses a system and method for generating a one-time password that changes pseudorandomly with each request for authentication. The method includes receiving a program-specific identifier (H(E)) from said program (E). The program specific identifier disclosed by Guski is the host application identifier (column 7 lines 28-32). Guski further discloses sending said program-password-specific identifier (F(H(E),p)) to said program (E), said program-password-specific identifier (F(H(E),p)) being processable by said program (E). The password (214) generated at the Security server (208) is sent to the client (202) where it is processed by creating the signon request (216) using specific ID.

Guski does not expressly disclose receiving said password (p); generating from at least said program-specific identifier (H(E)) and said received password (p) a program-password-specific identifier (F(H(E),p)).

However Abadi discloses creating passwords for password controlled access points (abstract). The method includes the user sending a master password (column 2 lines 64-65). The system disclosed by Abadi generates the passwords using a hard to invert function F to combine the user name, service name, and master password (column 3 lines 26-33).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to send a password from the client to the server of Guski to create the password as disclosed by Abadi. One of ordinary skill in the art would have been motivated to do this because users have to remember a large number of different passwords and creating passwords using a computerized method would reduce the number of passwords a user must remember and create more random, and therefore secure, passwords.

In reference to claim 6, Guski does not discloses a system wherein the program-password-specific identifier (F(H(E),p,s)) is generated from the program-specific identifier (H(E)), the received password (p), and an additional value (s), said additional value (s) characterizing a device (2) where the program-password-specific identifier (F(H(E),p,s)) is generated.

However Abadi discloses a system wherein the program-password-specific identifier (F(H(E),p,s)) is generated from the program-specific identifier (H(E)), the received password (p), and an additional value (s), said additional value (s) characterizing a device (2) where the program-password-specific identifier (F(H(E), p ,s)) is generated (Fig. 2). The additional value is the user name. The user name is characterizes the device because the device is used or owned by the user.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to send a password from the client to the server of Guski to create the password as disclosed by Abadi. One of ordinary skill in the art would have been motivated to do this because users have to remember a large number of different passwords and creating passwords using a computerized method would reduce the number of passwords a user must remember and create more random, and therefore secure, passwords.

Claim 2, 7, and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Guski and Abadi as applied to claim 1 above, and further in view of Schneier.

In reference to claims 2 and 11, Guski and Abadi do not disclose the program specific identifier derived by applying a first cryptographic function preferably a one-way hash function. Although Abadi discloses the second cryptographic function being a hard to invert function, where a one-way hash function is a hard to invert function, neither Guski not Abadi expressly disclose the second function being a one-way hash function, such as MD5 or SHA-1.

Schneier discloses the MD5 and SHA as hash functions that are used to create a hash value such that it is hard to find another pre-image message that produces the same hash value (page 429 paragraph 2); and therefore performs the function of H(E) of creating an identifier. Schneier further discloses the on-way hash function used to for security because the hash value is easy to compute, but difficult to reverse (page 429 paragraph 2).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the hash functions as disclosed by Schneier to create the identifier and a secure password in the system of Guski. One of ordinary skill in the art would have been motivated to do this because hash function prevent the substitution of a different pre-image message for the original pre-image message by providing a "fingerprint" of the pre-image.

In reference to claim 7, Guski and Abadi doe not disclose a system wherein the program-password-specific identifier (F(H(E),p)) is used as a key to decrypt another program.

Schneier discloses the use of a pass phrase (password) that is transformed into a random key by a one-way hash function (page 174 paragraph 2)

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the hash functions as disclosed by Schneier to create the identifier and a secure password in the system of Guski. One of ordinary skill in the art would have been motivated to do this because hash function prevent the substitution of a different pre-image message for the original pre-image message by providing a "fingerprint" of the pre-image.

Claims 3-5, and 12-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Guski and Abadi as applied to claim 1 above, and further in view of Cheng et al.

In reference to claim 3, Guski and Abadi do not disclose a system wherein a password-reading program (26) and the program-specific identifier (H(E)) are provided by means of a trusted computing base (TCB), preferably for both the same trusted computing base (TCB).

Cheng discloses a computer software architecture for distributed systems based on Trusted Computing Base program (Introduction page 216 paragraph 2).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the trusted computing base as in Cheng in the system of Guski. One of ordinary skill in the art would have been motivated to do this because TCB provides confidents that it enforces correctly a system security policy and satisfies some critical assurance criteria.

In reference to claim 4, Guski and Abadi do not disclose a system wherein the password (p) is received at the password-reading program (26), and, while said password-reading program (26) is executed, all I/O devices are locked and other programs are blocked.

Cheng discloses key distribution in a system based on TCB. One of the conditions required is that A and B believe that the key shared between them is secret shared exclusively (Section 4). Locking the I/O and blocking programs when the password is received ensures that only the trusted application A and trusted application B have the password.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the trusted computing base as in Cheng in the system of Guski. One of ordinary skill in the art would have been motivated to do this because TCB provides confidents that it enforces correctly a system security policy and satisfies some critical assurance criteria.

In reference to claims 5 and 12-13, Guski and Abadi do not disclose a system wherein the fact that the password-reading program (26) is executed based on the trusted computing base (TCB) is indicated via a signal, preferably by illuminating an LED (28), while the password-reading program (26) receives the password (p).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to indicate while the password-reading program receives the password in the system of Guski. One of ordinary skill in the art would have been motivated to do this because indicating will inform the user that a security process is in progress.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W Klimach whose telephone number is (703) 305-8421. The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (703) 305-4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

The 2100 Tech center will move to Carlyle in October 2004. The new telephone number for the receptionist is (571) 272-2100. The examiner's new telephone number will be (571) 272-3854.

Au 2135

PWK
Tuesday, August 31, 2004